AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Lisa A. Crandall, being duly sworn, depose and state as follows:

Introduction

1. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for warrants to search and seize the vehicle described in Attachment A1 – a white 2011 Ford Transit Van bearing Massachusetts registration 1HLB49 – for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2422(b) and 2252(a)(2) as set forth in Attachment B. The authorization sought includes permission to search any computer devices and electronic storage devices or media found in the van. For ease of reference, the van described in Attachment A1 is referred to below as the "TRANSIT VAN."

2. I have been employed as a Special Agent of the Federal Bureau of Investigation ("FBI") since June 2010. I am currently assigned to the FBI's Boston Division, Providence Resident Agency. As an FBI Special Agent, I have investigated federal criminal violations related to, among other things, the on-line sexual exploitation of children, white collar crime, and public corruption. Through my training and experience, I have become familiar with multiple types of digital devices and portable storage devices, to include but not limited to smartphones, computers, laptop computers, tablets, digital cameras, flash drives, USB drives, and external hard drives. In my experience as an FBI agent and former member of the FBI's Evidence Response Team, I have participated in the execution of dozens of search warrants that involved the handling of digital and portable storage devices and the collection of evidence from those devices.

3. The statements in this Affidavit are based in part on information provided by law enforcement officers employed by the Rhode Island West Warwick Police Department, FBI Special Agent Craig Graham, and my own investigation. This Affidavit does not set forth all of my knowledge about this matter. I have set forth only the facts that I believe are necessary to assess the existence of probable cause for the requested warrants.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 2422(b), enticement of a minor to engage in explicit sexual activity, and 18 U.S.C. § 2252(a)(2), receipt and distribution of child pornography (the "SUBJECT OFFENSES") occurred and that contraband, evidence, fruits, and instrumentalities of the aforementioned offenses – which are specified in Attachment B – will be found at the SUBJECT PREMISES and on the person of TORMEY.

Definitions

5. The following definitions apply to this Affidavit and its Attachments:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image of picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or

operating in conjunction with such device" and includes smartphones, mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

e. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer or other digital device to access the Internet. An IP address typically resembles four series of, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (ISPs) control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

h. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

i. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

j. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

k. "Mobile applications," as used herein, are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game.

l. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

m. "Remote Computing Service" ("RCS"), as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

n. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

o. A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, thumb drives, and other magnetic or optical media.

p. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

Probable Cause

6. On March 8, 2024, a resident of West Warwick reported to the West Warwick Police Department (hereinafter "WWPD") that her minor daughter had been sexually assaulted by an adult male on or around December 30, 2023. The minor was identified as a 14-year-old female born in 2009 (hereinafter "MINOR 1").

7. Law enforcement officers spoke with MINOR 1's mother, and MINOR 1 was interviewed by both a physician at the Aubin Center in Providence, and a Forensic Interviewer at the FBI Providence office. Officers learned from MINOR 1 that in or around December of

2023, she communicated with an individual through the mobile application TikTok[1] and sent the individual multiple images of herself nude (in full or in part) and one video of herself nude (in full or in part) at the individual's request. MINOR 1 specified that she sent those images and that video using a social media application. MINOR 1 later identified the individual's TikTok account as having a display name of "tacobell999$$$" and a username of "@tacobell99948." MINOR 1 advised that she communicated with the same individual on Instagram[2] and identified the individual's Instagram account as either "kwakle" or "kwaxle."

8. I note based on my experience and training that the use of social media applications to transmit and/or receive image or video files involves the transmission of data over the Internet and/or interstate lines of communication and accordingly involves a means or facility of interstate commerce.

9. MINOR 1 provided her own account information for the accounts that she used to communicate with the individual to law enforcement during her forensic interview. She provided her TikTok account as "juvajanga" and her Instagram account as "2fine4youbbyyy."

10. Preservation letters for all of these accounts were sent to the respective social media companies.

[1] TikTok is a social media application developed and owned by Chinese Internet company ByteDance. TikTok is a short-form video hosting service which allows users to view and post short videos. Users can also comment on videos and directly message other users. The application uses the device's data plan or Wi-Fi to transmit and receive content.

[2] Instagram is a social media application developed and owned by Meta Platforms, Inc. Instagram allows users to view and post images. Users can also comment and directly message other users. The application uses the device's data plan or Wi-Fi to transmit and receive content.

11. MINOR 1 also disclosed to the interviewers that on or about December 30, 2023, she snuck out of her mother's house to meet the same individual in person. The individual also communicated that he wanted to pay MINOR 1 $200 to let him perform oral sex on her.

12. I know through my training and experience that TikTok and Instagram are social media applications that are commonly accessed using a cell phone. MINOR 1 stated that the individual who communicated with her through those social media applications, also communicated with her while he was traveling to meet her.

13. MINOR 1 described the individual she met as having long brown hair, a brown beard, and wearing glasses. In her conversations with the individual in person and online, he stated that he was from Newport, RI, was 29 years old, and was named "Pat." MINOR 1 stated that she may have initially told Pat that she was 16, but that she later communicated and he understood that she was 14 years old.

14. MINOR 1 described the vehicle Pat arrived in as a white van which had the rear seats removed. MINOR 1 first sat in the front passenger seat of the van while talking to Pat. They then moved to the back of the van, where Pat pulled up MINOR 1's sweatshirt and kissed her chest. Pat then pulled her sweatpants and underwear down, and his lips and tongue touched her vagina. Pat's penis and fingers also touched the inside of MINOR 1's vagina. At the end of the encounter, Pat gave MINOR 1 two hundred dollars.

15. WWPD obtained consent to search MINOR 1's cell phone. An extraction of the phone's contents was performed and the results of the extraction was reviewed by FBI Providence. The telephone number associated with MINOR 1's device was found to be 401-545-6807. MINOR 1's mother advised law enforcement that she had been in control of MINOR 1's

phone since approximately February 9, 2024. Prior to that time, MINOR 1 had blocked @tacobell99948's account. MINOR 1's mother unblocked @tacobell99948 and communicated with the account through MINOR 1's TikTok account. MINOR 1's mother said that she engaged in the communications to learn more about the user of @tacobell99948.

16. A review of the cellphone extraction for images identified multiple images of what appear to be MINOR 1 disrobed. The images depict what appears to be MINOR 1's nude torso, including her breasts and vulva. The images appear to be taken by MINOR 1 using a mirror. This review did not include a review of image transmission information.

17. A review of the cellphone extraction identified communications from February 21, 2024 to March 10, 2024 between MINOR 1's TikTok account (which at the time was being used by MINOR 1's mother) and TikTok account @tacobell99948. In the following communications @tacobell99948 communicated that he wanted to have sexual relations with MINOR 1:

02/22/2024 - 3:35pm	MINOR 1's account	still tryna link?
02/22/2024 - 3:36pm	@tacobell99948	Ya hbu Thinkin bout u m
02/22/2024 - 3:39pm	MINOR 1's account	Wat you thinkin about
02/22/2024 - 3:39pm	@tacobell99948	Smashin u
02/22/2024 - 3:41pm	MINOR 1's account	tell me more
02/22/2024 - 3:42pm	@tacobell99948	Ur right lll bod Wanna eat u out
02/22/2024 - 3:39pm	MINOR 1's account	Wat you thinkin about
02/22/2024 - 3:39pm	@tacobell99948	Smashin u
02/22/2024 - 3:41pm	MINOR 1's account	tell me more

02/22/2024 - 3:42pm	@tacobell99948	Ur right lll bod Wanna eat u out Taste u Wanna smash u so bad m U like? lol u rly busy rn it ok
03/08/2024 - 3:42pm	@tacobell99948	[a link was sent which was no longer accessable]
03/10/2024 - 6:20pm	@tacobell99948	Wanna link wid u

18. Consent was also obtained to search MINOR 1's iPad. An extraction of the iPad's contents was performed and images obtained through the extraction were reviewed by FBI Providence. That review found a video that depicts a female inserting a toothbrush handle into her vagina. The video shows only the female's vagina and hand. That review did not include a review of video transmission information.

19. A subpoena was issued to TikTok for account information related to the account @tacobell99948. TikTok provided the following subscriber information:

Username: tacobell99948

Signup Device Info: iPhone15,4

Signup date 01/03/2024 05:25:13am (UTC)

Phone number: +14013740760

Email: drewdrewdrew134@yahoo.com

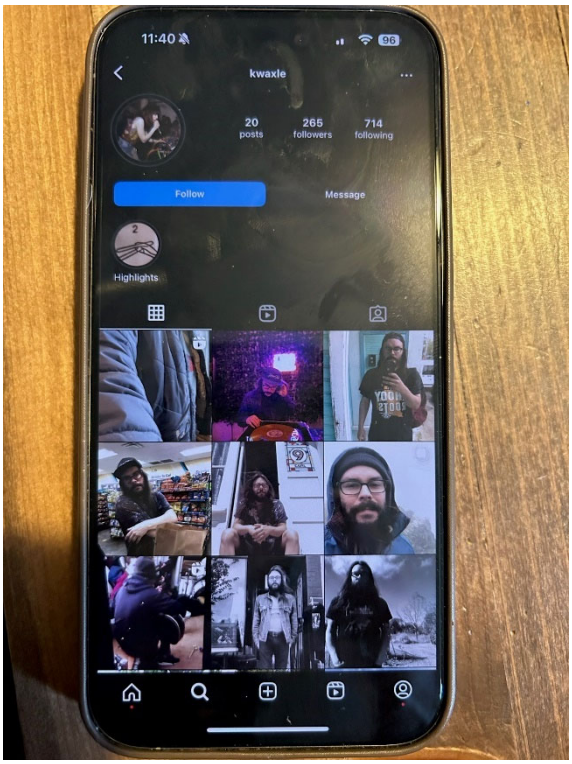
TikTok also provided IP Session history, the most common IP addresses returned were 68.9.40.11, 68.9.40.92, and 98.175.157.68.

20. Cox Communications was subpoenaed and provided subscriber information for the IP addresses. 68.9.40.11 and 68.9.40.92 returned to Robert Tormey, 38 Top O The Mark

Drive, Jamestown, Rhode Island 02835. 98.175.157.68 returned to Vinyl Guru Record Shop at 154 Broadway, Newport, RI 02840, and Cox records further indicated a telephone number of 401-374-0760 and an email address of vinylgururecordshop@gmail.com.

21. MINOR 1's mother also provided law enforcement with a screen shot of the Instagram account "kwaxle." MINOR 1's mother obtained the screen shot by navigating to the Instagram account using her own cellular telephone. MINOR 1's mother found the kwaxle account based on MINOR 1's recollection of the account's name and MINOR 1 later identified the adult male depicted in the screen shot as Pat, the individual she had sexual relations with on or about December 30, 2023.

22. WWPD was able to identify the individual depicted in the kwaxle account as Kyle Patrick TORMEY, born in 1984. A search of law enforcement databases indicated that TORMEY's home address was 19 Caleb Earl Street, Newport, Rhode Island. A comparison of TORMEY's driver's license photo indicated that TORMEY was the individual depicted on the kwaxle account. The kwaxle account also displayed an image of TORMEY sitting in front of a door that was identified as the front door to 19 Caleb Earl Street, Newport, Rhode Island. Below are images of the kwaxle account and TORMEY's driver's license photo:



23. A subpoena was issued to Instagram for account information related to the account kwaxle. Subscriber information for the account indicated a verified email address of kwaxledelic@gmail.com. A subpoena was then issued to Google for account information related to kwaxledelic@gmail.com and the following subscriber information was returned:

Name: kyle bobyle

Recovery email: kylesantiques@gmail.com

24. A subpoena issued to Google for account information related to kylesantiques@gmail.com returned the following subscriber information:

Name: kyle tormey

Recovery email: vinylgururecordshop@gmail.com

Recovery SMS: +4013740760

25. Open-source searches indicated that TORMEY is an owner/operator of Vinyl Guru Record Shop located at 154 Broadway, Newport, RI 02840 and that telephone 401-374-0760 is associated with Vinyl Guru Record Shop on multiple websites. Surveillance on March 14, 2024 observed TORMEY entering and exiting Vinyl Guru Record Shop located at 154 Broadway, Newport, Rhode Island, and observed posted business hours of the shop as 12pm to 6pm. The telephone number associated with Vinyl Guru Record Shop is the same number included in the subscriber information for TikTok account @tacobell99948, the same telephone number associated with Vinyl Guru Record Shop's IP address, and the same telephone number in the subscriber information for the recovery email address of the email used to create Instagram account kwaxle. The TikTok communications which occurred between MINOR 1's account and @tacobell99948 occurred during the posted business hours of the Vinyl Guru Record Shop.

26. A subpoena issued to Verizon for account information related to telephone number 401-374-0760 returned information indicating that account was associated with Mary Tormey of Swansea, Massachusetts. A law enforcement database indicated that Kyle TORMEY's mother's name is Mary Tabor. A search of Department of Motor Vehicle records indicated that Mary Tabor has an alias of Mary Tormey and lives at the same Swansea, MA, address as that associated with telephone number 401-374-0760.

27. Department of Motor Vehicles records also indicated that a white 2011 Ford, Massachusetts registration 1HLB49, is registered to Mary Tabor at the same Swansea, MA, address. Law enforcement records described the 2011 Ford as a transit van. Subpoenaed

records from the Rhode Island Turnpike and Bridge Authority indicated that 1HLB49 traveled Westbound over the Newport Bridge at approximately 6:55pm on December 30, 2023, and returned Eastbound over the Newport Bridge at approximately 12:11am on December 31, 2023.

28. Surveillance conducted on March 14, 2024, observed TORMEY sitting in the open doorway of 19 Caleb Earl Street smoking a cigarette. Additionally, a subpoena issued to Rhode Island Energy returned customer information indicating that TORMEY has an active electric and gas account for 19 Caleb Earl Street with a provided customer telephone number of 401-374-0760.

29. Surveillance conducted on April 4, 2024, observed TORMEY opening Vinyl Guru Record Shop at 12:23pm for approximately one minute before locking the door and returning to 19 Caleb Earl Street. TORMEY then returned at 12:50pm and re-opened the shop. At approximately 1pm, a law enforcement officer entered the shop and observed TORMEY as the sole employee present. A laptop computer and cell phone were also observed sitting on the counter within the business.

30. Surveillance conducted on the morning of April 17, 2024 observed the TRANSIT VAN parked along the street immediately in front of 19 Caleb Ear Street.

31. Based on the above, I believe that there is probable cause to believe that the TRANSIT VAN is the white van that MINOR 1 identified, as described in paragraph 14 above, and is a vehicle used by TORMEY.

Characteristics Common to Individuals Who
Collect or Traffic Child Pornography

32. Based on my previous investigative experience related to child exploitation investigations and the training and experience of other law enforcement officers with whom I

have had discussions, I know there are certain characteristics common to individuals who distribute, receive, possess, and/or access with intent to view material which depicts minors engaged in sexually explicit conduct. Said material may include, but is not limited to, photographs, negatives, slides, magazines, printed media, motion pictures, video tapes, books and other media stored electronically on computers, digital devices or related digital storage media.

33. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

34. Such individuals often view their child pornographic materials as valuable commodities, sometimes even regarding them as prized collections. Subsequently, these individuals prefer not to be without their child pornographic material for any prolonged period of time and often go to great lengths to conceal and protect their illicit collections from discovery, theft, or damage. To safeguard their illicit materials, these individuals may employ the following methods:

a. The use of Internet-based data storage services, such as Google Drive.

b. The use of labels containing false, misleading or no title.

c. The application of technologies, software, and other electronic means such as encryption, steganography (the practice of concealing a file, message, image, or video

within another file, message, image or video), partitioned hard drives, and misleading or purposefully-disguised applications on electronic devices.

d. The use of safes, safety deposit boxes, or other locked or concealed compartments within premises or structures that the individual controls.

35. Based on my training and experience, it is typical of individuals involved in child pornography to be initially reluctant to admit possessing child pornography or be willing to share such materials with other individuals online. Sometimes individuals falsely and or inaccurately claim they deleted "all" of their child pornography collections. Often, such individuals maintain child pornography on a variety of different media and continue to keep child pornography even when some such materials are "deleted." This is particularly true of individuals who have distributed child pornography in the past.

36. Likewise, such individuals often maintain their collections for several years and keep them close by, usually at the possessor's residence, inside the possessor's vehicle, or on their persons, to enable the individual to view the child pornography images. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

37. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.[3]

[3] *See United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because "staleness inquiry must be grounded in an understanding of both the behavior

38. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

Background on Child Pornography, Computers, and the Internet

39. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and smartphones with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

---

of child pornography collectors and of modern technology"); *see also United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370–71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010).)

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively, and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types – to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices which are plugged into a port on the computer – can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide e-mail services and/or electronic storage of computer files in any

variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in many cases.

g. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

Specifics of Search and Seizure of Computer Devices

40. As described above and in Attachment B, this application seeks permission to search for records that might be found at the SUBJECT PREMISES and/or on the person of TORMEY, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

41. I submit that if a computer or storage medium, including a smart phone, is found at the SUBJECT PREMISES or on the person of TORMEY, there is probable cause to believe

those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

40. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium at the SUBJECT PREMISES or on the person of TORMEY because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to

establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a

digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic

programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

44. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware

and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software website, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data

within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

45. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

46. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

Probable Cause for Search of Transit Van

47. As described above, I believe that there is probable cause to believe that TORMEY communicated in furtherance of the SUBJECT OFFENSES with MINOR 1 using a computer device (which includes a desktop computer, tablet computer, and smartphone). As described above, there is probable cause to believe that such a device would be stored in a safe space or space over which TORMEY has control. Such places would include any vehicle that TORMEY uses, including the TRANSIT VAN. Furthermore, common sense and ordinary experience advise that owners of computer devices may keep them stored, at least temporarily, in vehicles that they use, which in TORMEY's case would be the TRANSIT VAN.

48. Ordinary experience indicates that paper and/or electronic records pertinent to tying TORMEY to his computer devices, cellular telephones, his parents and their residences, the white van MINOR 1 described, his business, his TikTok and Instagram accounts, the white 2011 Ford registered in his mother's name (namely the TRANSIT VAN), his familiarity with MINOR 1, and passwords associated with his social media accounts and computer devices will be found in the TRANSIT VAN and/or on computer devices and electronic storage devices or

media that would be found in the TRANSIT VAN. More generally, all of the items described in Attachment B as items to be seized are materials or records that constitute contraband, evidence, fruits, or instrumentalities of the SUBJECT OFFENSES, and based on my investigative experience, ordinary experience, and common sense such materials and records are likely to be found in the TRANSIT VAN.

Conclusion

49. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein, the SUBJECT OFFENSES, have been violated, and that the contraband, property, evidence, fruits, and instrumentalities of these offenses, more fully described in Attachment B, are located at the vehicle described in Attachments A1, namely the TRANSIT VAN. I respectfully request that this Court issue a search warrant for the vehicle described in Attachment A1 authorizing the seizure and search of the items described in Attachment B.

50. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Sworn to under the pains and penalties of perjury,

Lisa A. Crandall
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by _____
(specify reliable electronic means)

_____ _____
Date *Judge's signature*

_____ _____
City and State *Magistrate Judge Patricia A. Sullivan*

ATTACHMENT A1

DESCRIPTION OF LOCATION TO BE SEARCHED

The vehicle to be searched is a while Ford 2011 transit van bearing Massachusetts registration 1HLB 49. This vehicle is located in Newport, Rhode Island. On the morning of April 16, 2023, this vehicle was seen parked on Caleb Earl Street in Newport in front of the residence at 19 Caleb Earl Street, and it is anticipated that this vehicle will remain at this location at the time of any search and seizure that is authorized pursuant to warrant.

Below are two color photographs of the vehicle as seen on the morning of April 16, 2023.


17
15
9
TRANSIT

ATTACHMENT B

Description of Items to be Searched

1. Computer(s), computer hardware, computer software, cellular telephones, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; display or access communications with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs, including, but not limited to, P2P software.

3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, access with intent to view, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, access with intent to view, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or the employment, use, persuasion, inducement, enticement, or coercion of any minor to engage in sexually explicit conduct.

4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

5. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, production, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals (including minors) about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and

electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

9. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

11. Any and all cameras, film, videotapes or other photographic equipment.

12. Any and all visual depictions of minors.

13. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child

pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

14. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

15. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

16. Credit card information, including, but not limited to, bills and payment records.

17. Records or other items which evidence ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

18. Routers, modems, and network equipment used to connect computers to the Internet.

Description of Items to Be Seized

1. Computer(s), computer hardware, computer software, cellular telephones, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information

pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs, including, but not limited to, P2P software.

3. Any and all notes, documents, invoices, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, handwritten notes, other digital data files and web cache information) that:

a. Pertains to the possession, access with intent to view, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8);

b. Pertains to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2);

c. Identifies persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2);

d. Contains or references communications between individuals (including minors) about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.

e. Indicates, references, or otherwise tends to show memberships in online groups, clubs, or services that provide or make accessible child pornography to members.

f. Addresses accounts with an Internet Service Provider, including but not limited to Comcast.

g. Pertains to online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

h. Indicates occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.

i. Indicates or evidences ownership or use of computer equipment found in the above residence, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

4. Any and all cameras, film, videotapes, or other photographic equipment.

5. Any and all visual depictions of minors.

6. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

7. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or

foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual 12 3:22-mj-00045 depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

8. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

9. Routers, modems, and network equipment used to connect computers to the Internet.

As used in Attachment B, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to

law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.